Ben Steinberg (*pro hac vice*)
Kellie Lerner (*pro hac vice* forthcoming)
ROBINS KAPLAN LLP
1325 Avenue of the Americas, Suite 2601
New York, NY 10019
Telephone: (212) 980-7400
Facsimile: (212) 980-7499
klerner@robinskaplan.com
bsteinberg@robinskaplan.com

Christian Levis (admitted *pro hac vice*)
Amanda Fiorilla (admitted *pro hac vice*)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

[Additional counsel on signature page]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

DARIUS CLARK, JOHN H. COTTRELL, DAVID LUMB, KYLA ROLLIER and JENNY SZETO, individually and on behalf of all others similarly situated,

Plaintiff,

v.

YODLEE, INC., a Delaware corporation,

Defendant.

Case No. 3:20-cv-5991 (SK)

THIRD AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

SUMMARY OF ALLEGATIONS **1**

JURISDICTION AND VENUE **4**

PARTIES **5**

I. Plaintiffs 5

II. Defendant 7

FACTUAL ALLEGATIONS **7**

I. The Founding of Yodlee 7

II. Envestnet | Yodlee Collects and Sells Individuals' Financial Data Without Their Consent 9

III. Envestnet | Yodlee Stores Consumers' Data for Backup Purposes 15

IV. Envestnet | Yodlee's Failure to Disclose Violates Several Privacy Laws 16

V. Government and Industry Leaders Agree that Yodlee's Conduct Is Wrong, Risky, Dangerous and Bad for Consumers 20

VI. Plaintiffs and Class Members Lost Indemnification Rights and Other Rights and Protections 23

VII. Plaintiffs and Class Members Lost Control Over Valuable Property and the Ability to Receive Compensation for It 24

VIII. Plaintiffs and Class Members Suffered an Increased Risk of Identity Theft and Fraud 26

IX. Plaintiffs and Class Members Have a Reasonable Expectation of Privacy 27

X. Yodlee Lacks Adequate Safeguards to Protect Consumers' Data 28

XI. Members of Congress Requested an FTC Investigation into Yodlee's Practices 32

TOLLING, CONCEALMENT AND ESTOPPEL **33**

PLAINTIFFS LACK AN ADEQUATE REMEDY AT LAW **34**

CLASS ACTION ALLEGATIONS **36**

CALIFORNIA LAW APPLIES TO THE NATIONWIDE CLASS **38**

CLAIMS FOR RELIEF **39**

Darius Clark, John H. Cottrell, David Lumb, Kyla Rollier and Jenny Szeto (together, "Plaintiffs"), on behalf of themselves and all others similarly situated, assert the following against Defendant Yodlee, Inc. ("Yodlee" or "Envestnet | Yodlee"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

SUMMARY OF ALLEGATIONS

1. The Internet age has spawned the development of a vast data economy. Among its key players are data harvesters, companies that collect and repackage data from various sources for sale to advertisers, investors, researchers, and other third parties.

2. Envestnet | Yodlee is one of the largest such companies in the world. Its business focuses on harvesting highly sensitive financial data—such as bank balances, credit card purchase details, loan information, and other transaction histories—from individuals throughout the United States and then selling it to Yodlee's "data and analytics" customers.

3. This data is not available from public sources and is so sensitive that the individuals it concerns would not voluntarily turn it over. Instead, Yodlee acquires it by deceit.

4. Envestnet | Yodlee surreptitiously collects such data from software products—either application programming interfaces ("APIs"), software development kits ("SDKs"), or both—that it markets and sells to some of the largest financial institutions in the country. These institutions include the nation's 15 top banks (e.g., Bank of America, Merrill Lynch, and Citibank), 10 top wealth management firms, and digital payment platforms like PayPal.

5. Envestnet | Yodlee, in turn, acquires financial data about each individual that interacts with the software installed on its customers' systems. However, these individuals often have no idea they are dealing with Envestnet | Yodlee.

6. This is by design. Given the highly sensitive nature of the data that Envestnet | Yodlee collects, its software is developed to be seamlessly integrated directly into the host company's existing website and/or mobile app in a way that obscures whom the individual is dealing with and where their data is going. For example, when individuals connect their bank accounts to PayPal, they are prompted to enter their credentials into a log in screen that mirrors what they would see if they directly logged into their respective bank's website. Their financial

institution's logo is prominently displayed on each of the screens that they interact with and the individuals use the same usernames and passwords they would use to log in to their financial institution's own website or mobile app. At no point are the individuals prompted to create or use an Envestnet | Yodlee account.

7. Moreover, to the extent Envestnet | Yodlee is mentioned, individuals are not given accurate information about what Envestnet | Yodlee does or how it collects their data. For example, PayPal discloses to individuals that Envestnet | Yodlee is involved in connecting their bank account to PayPal's service for the limited purpose of confirming the individual's bank details, checking their balance, and transactions, "as needed." While this might be true for that initial log in, Envestnet | Yodlee's involvement with the individual's data goes well beyond the limited consent provided to facilitate a connection between their bank account and PayPal.

8. From the moment of that initial linkage, unbeknownst to consumers, Envestnet | Yodlee obtains 90 days of transaction history—including all details about every purchase the user made in that period, no matter how intimate, as well as biographic and demographic data. And even if a user only connects a particular account to the app, such as her checking account, Envestnet | Yodlee will take information from *all* accounts linked to those credentials, including checking, savings, credit, loan, and even retirement or brokerage accounts.

9. In fact, Envestnet | Yodlee stores a copy of each individual's bank log in information (i.e., her username and password) on its own system *after* the connection is made between that individual's bank account and any other third party service (e.g., PayPal). Envestnet | Yodlee then exploits these credentials to routinely extract data from that user's accounts without consent, even when there is no PayPal transaction at issue. Yodlee uses that data to construct individualized profiles for millions of Americans, and they profit by selling access to that data in the form of large text files containing data on specific transactions for millions of users.

10. This process continues even if, for example, an individual severs the connection between its bank account and the third-party service (e.g., PayPal) that Envestnet | Yodlee facilitated. In that instance, Envestnet | Yodlee relies on its own stored copy of the individual's credentials to extract financial data from her accounts long after the access is revoked.

11. As U.S. Senator Ron Wyden explained to the Federal Trade Commission ("FTC") in a letter concerning Envestnet | Yodlee's practices, this unagreed-to data collection is particularly problematic because, "[c]onsumers' credit and debit card transactions can reveal information about their health, sexuality, religion, political views, and many other personal details."[1] It is no wonder that Envestnet | Yodlee has been highly successful as, according to the *Wall Street Journal*, companies are willing to pay as much as $4 million a year for access to this sort of highly personal data.

12. Plaintiffs connected their bank accounts to PayPal using an Envestnet | Yodlee-powered portal in order to facilitate transfers among those accounts. At no time was it disclosed by PayPal, Yodlee, or Plaintiffs' banks, that Yodlee would continuously access Plaintiffs' accounts to extract and sell data without their consent.

13. Yodlee also fails to take reasonable precautions to protect the highly sensitive data they collect from individuals without authorization. Yodlee makes the data available to its data and analytics customers as large text files containing data on specific transactions, each traceable to a particular user because it is labeled by a "Yodlee-specific identifier." Yodlee distributes this data in unencrypted plain text files. Users and developers have raised concerns about this practice. These files, which can be read by anyone who acquires them, contain highly sensitive information that make it possible to identify the individuals involved in each transaction.

14. Yodlee's failure to take even the most basic steps to protect this highly sensitive data (e.g., requiring a password to open such files) has caused Plaintiffs and Class members significant harm. While Yodlee claims to only acquire, use or disclose data after receiving the "necessary permissions," Envestnet | Yodlee makes no disclosures to consumers itself, instead relying on third party apps like PayPal to disclose Envestnet | Yodlee's practices. Prior to its acquisition by Envestnet, Yodlee admitted in filings with the United States Securities and Exchange Commission ("SEC") that it "does not audit its customers to ensure that they have acted, and continue to act,

---

[1] Letter from Sen. Ron Wyden et al., Cong. of the U.S., to Joseph J. Simons, Chairman, Fed. Trade Comm'n (July 31, 2020), https://www.wyden.senate.gov/imo/media/doc/073120%20Wyden%20Cassidy%20Led%20FTC%20Investigation%20letter.pdf.

consistently with such assurances."[2] Envestnet | Yodlee, accordingly, cannot guarantee Plaintiffs or other Class members that its clients, or anyone with whom its clients share Class members' sensitive personal data, are not using such data for nefarious purposes.

15. Plaintiffs and Class members suffered actual harm, injury, damage and loss as a result of Yodlee's illegal conduct, including, but not limited to economic damages and harm to their dignitary rights.

16. Yodlee has deprived Plaintiffs and Class members of indemnification rights and other rights and protections they enjoyed as long as their data remained in the protected banking environment. Yodlee also has deprived Plaintiffs and Class members of control over their valuable property (namely, their sensitive personal data), including the ability to receive compensation for that data and the ability to withhold their data for sale.

17. Yodlee's practices and conduct have subjected Plaintiffs and Class members to an increased risk of identity theft and fraud.

18. Had Plaintiffs and Class members known the true nature, significance and extent of Yodlee's data practices, they would not have used Envestnet | Yodlee.

JURISDICTION AND VENUE

19. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative members of the Classes defined below, and a significant portion of putative Class members are citizens of a state different from Yodlee.

20. This Court has general personal jurisdiction over Envestnet | Yodlee because Envestnet | Yodlee's principal place of business is in Redwood City, California.

21. Venue is proper in this District pursuant to 28 U.S.C. §1391(b), (c), and (d) because Yodlee transacts business in this District; a substantial portion of the events giving rise to the claims occurred in this District; and because Yodlee is headquartered in this District.

---

[2] Yodlee, Inc., Proxy Statement/Prospectus, (Oct. 21, 2015), https://www.sec.gov/Archives/edgar/data/1337619/000104746915007906/a2226277z424b3.htm.

22. Intra-district Assignment: A substantial part of the events and omissions giving rise to the violations of law alleged herein occurred in the County of San Mateo, and as such, this action may be properly assigned to the San Francisco or Oakland divisions of this Court pursuant to Civil Local Rule 3-2(c).

PARTIES

I. PLAINTIFFS

23. Plaintiff **Darius Clark** is a natural person, a citizen of the State of Ohio and a resident of Hamilton County.

24. Mr. Clark is a PayPal user who connected his Alliant Credit Union, UMB/Fidelity, and BBVA Simple accounts to PayPal through Envestnet | Yodlee's API in order to facilitate transfers among those accounts. At no time was it disclosed by PayPal, Yodlee, Alliant Credit Union, UMB/Fidelity, or BBVA Simple that Envestnet | Yodlee would retain a copy of his credentials and continuously access Mr. Clark's accounts to extract data. Yodlee collected, retained, and sold Mr. Clark's data without his knowledge or consent. On information and belief, at the time that Mr. Clark linked his accounts to PayPal, Envestnet | Yodlee obtained—without his knowledge or authorization—90 days' worth of detailed transaction history from all accounts connected to his credentials, and continues to supplement that data on an ongoing basis by collecting new data from Plaintiff Clark's accounts.

25. Plaintiff **John H. Cottrell** is a natural person, a citizen of the State of Texas and a resident of Collin County.

26. Mr. John Cottrell is a PayPal user who connected his BBVA Bank account to PayPal through Envestnet | Yodlee's API in order to facilitate transfers among those accounts. At no time was it disclosed by PayPal, Yodlee, or BBVA Bank that Envestnet | Yodlee would retain a copy of his credentials and continuously access Mr. John Cottrell's accounts to extract data. Yodlee collected, retained, and sold Mr. John Cottrell's data without his knowledge or consent. On information and belief, at the time that Mr. John Cottrell linked his account to PayPal, Envestnet | Yodlee obtained—without his knowledge or authorization—90 days' worth of detailed transaction history from all accounts connected to his credentials, and continues to supplement that data on an

ongoing basis by collecting new data from Plaintiff John Cottrell's accounts.

27. Plaintiff **David Lumb** is a natural person, a citizen of the State of Tennessee and a resident of Shelby County.

28. Mr. Lumb is a PayPal user who connected his Commercial Bank & Trust account to PayPal through Envestnet | Yodlee's API in order to facilitate transfers among those accounts. At no time was it disclosed by PayPal, Yodlee, or Commercial Bank & Trust that Envestnet | Yodlee would retain a copy of his credentials and continuously access Mr. Lumb's accounts to extract data. Yodlee collected, retained, and sold Mr. Lumb's data without his knowledge or consent. On information and belief, at the time that Mr. Lumb linked his account to PayPal, Envestnet | Yodlee obtained—without his knowledge or authorization—90 days' worth of detailed transaction history from all accounts connected to his credentials, and continues to supplement that data on an ongoing basis by collecting new data from Plaintiff Lumb's accounts.

29. Plaintiff **Kyla Rollier** is a natural person and citizen of the State of Florida and a resident of Volusia County.

30. Ms. Rollier is a PayPal user who connected her Launch Credit Union account to PayPal through Envestnet | Yodlee's API in order to facilitate transfers among those accounts. At no time was it disclosed by PayPal, Yodlee, or Launch Credit Union that Envestnet | Yodlee would retain a copy of her credentials and continuously access Ms. Rollier's accounts to extract data. Yodlee collected, retained, and sold Ms. Rollier's data without her knowledge or consent. On information and belief, at the time that Ms. Rollier linked her account to PayPal, Envestnet | Yodlee obtained—without her knowledge or authorization—90 days' worth of detailed transaction history from all accounts connected to her credentials, and continues to supplement that data on an ongoing basis by collecting new data from Plaintiff Rollier's accounts.

31. Plaintiff **Jenny Szeto** is a natural person and citizen of the State of California and a resident of San Francisco County.

32. Ms. Szeto is a PayPal user who connected her J.P. Morgan Chase account to PayPal through Envestnet | Yodlee's API in order to facilitate transfers among those accounts. At no time was it disclosed by PayPal, Yodlee, or J.P. Morgan Chase that Envestnet | Yodlee would retain a

copy of her credentials and continuously access Ms. Szeto's accounts to extract data. Yodlee collected, retained, and sold Ms. Szeto's data without her knowledge or consent. On information and belief, at the time that Ms. Szeto linked her account to PayPal, Envestnet | Yodlee obtained—without her knowledge or authorization—90 days' worth of detailed transaction history from all accounts connected to her credentials, and continues to supplement that data on an ongoing basis by collecting new data from Plaintiff Szeto's accounts.

II. DEFENDANT

33. Defendant Yodlee, Inc. is a Delaware corporation with principal executive offices located at 3600 Bridge Parkway, Suite 200, Redwood City, CA 94065.

FACTUAL ALLEGATIONS

I. THE FOUNDING OF YODLEE

34. Yodlee was founded in 1999. Initially, Yodlee was focused on providing banks and financial institutions with software that would improve the user experience, for example, making it possible for banking clients to view bank statements, financial accounts, and investment portfolios all at once without relying on multiple logins or webpages.

35. Yodlee later expanded its business to develop APIs for financial apps and software (collectively, "FinTech Apps"). This includes payment apps, such as PayPal; personal budgeting apps, such as Personal Capital; and apps for particular banks. Envestnet | Yodlee's software silently integrates into its clients' existing platforms to provide various financial services, like budgeting tools, savings trackers, or account history information. In each instance, the customer believes that she is interacting with her home institution (e.g., her bank) and has no idea she is logging into or using an Envestnet | Yodlee product.

36. Yodlee profits from these interactions in two ways. First, the financial institutions that use Yodlee's software pay a licensing fee to integrate Envestnet | Yodlee's API into their platform. Second, Envestnet | Yodlee collects the financial data of each individual that connects to one of the FinTech Apps through a bank or other financial institution using its software. This information, which includes an individual's bank account balances, transaction history and other

data, is then compiled into a large data set with that of other individuals and sold to third parties for a fee.

37. Envestnet | Yodlee's reach and the amount of data it collects is extraordinary. More than 150 financial institutions and a majority of the 20 largest U.S. banks integrate Yodlee's API into their platforms. According to filings with the SEC, more than 900 companies subscribe to the Yodlee platform to power customized FinTech Apps and services for millions of their users.

38. Given its widespread success, Yodlee went public on NASDAQ in October of 2014, generating almost $100 million that year. Prior to its public offering, Yodlee claims it only provided data to third parties for "research uses," such as "enhanc[ing] predictive analysis."

39. In 2015, Yodlee was acquired by Envestnet. The deal valued Yodlee at $590 million or approximately $19 per share. The acquisition was considered the second largest FinTech deal in U.S. history at the time.

40. That same year, the *Wall Street Journal* released a report revealing for the first time that a large part of Yodlee's revenue was actually generated by a different lucrative source: selling user data. The report concluded that Yodlee has been selling data it gathers from users for at least the last year.

41. Yodlee denied the *Wall Street Journal* report, claiming it had only "a very limited number of partnerships with firms to develop . . . sophisticated analytics solutions." Yodlee claimed these partners only received "a small, scrubbed, de-identified, and dynamic sample of data to enable trend analysis. Yodlee does not offer, nor do partners receive, raw data." But, as discussed below, these statements were false.

42. Currently, Yodlee sells sensitive personal data of tens of millions of individuals to a large customer base, including investment firms and some of the largest banks in the United States, like J.P. Morgan.[3] One of Envestnet | Yodlee's products, called its "Data Platform," offers "the best and most comprehensive financial data at massive scale across retail banking, credit, and wealth

[3] Joseph Cox, *Leaked Document Shows How Big Companies Buy Credit Card Data on Millions of Americans*, Vice, (Feb. 19, 2020), https://www.vice.com/en/article/jged4x/envestnet-yodlee-credit-card-bank-data-not-anonymous.

management." Envestnet | Yodlee explains "[t]his is made possible through the strengths of our data acquisition capabilities, extensive data cleaning and enrichment expertise, and massive scale."[4]

43. Yodlee's conduct violates Plaintiffs' and Class members' privacy rights and several state and federal laws because, as explained below, Yodlee collects and sells Plaintiffs' and Class members' highly sensitive personal data without their knowledge or consent. Furthermore, Envestnet | Yodlee fails to implement adequate security measures to protect Plaintiffs' and Class members' data, leaving their highly sensitive personal data vulnerable to hackers, criminals, and other unauthorized third parties.

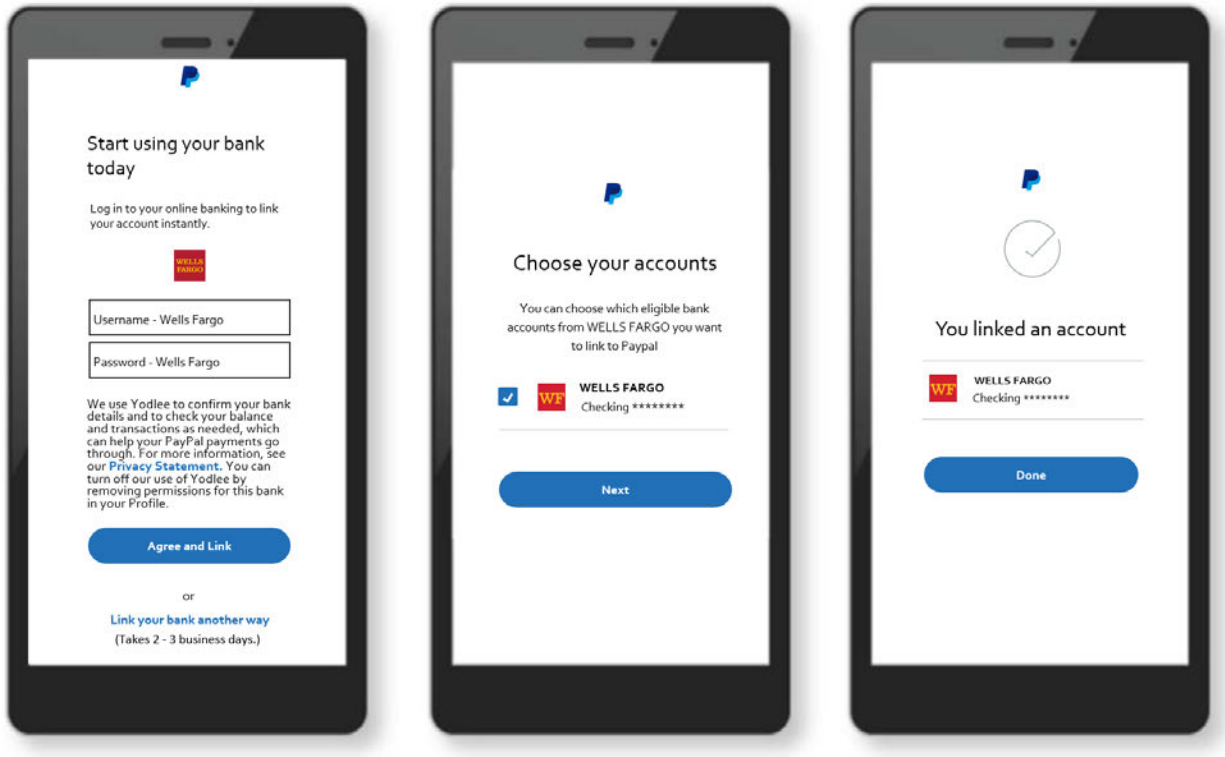
II. ENVESTNET | YODLEE COLLECTS AND SELLS INDIVIDUALS' FINANCIAL DATA WITHOUT THEIR CONSENT

44. While Envestnet | Yodlee claims that it only sells "small . . . sample[s] of data," in reality, Yodlee sells millions of users' sensitive personal data to hundreds of clients. As explained below, this data is collected without the individual's consent by leveraging credentials provided to Envestnet | Yodlee for a different, specific, and limited purpose.

45. For example, PayPal uses Envestnet | Yodlee's account verification API to validate an individual's bank account so that the individual can use that account with PayPal's services. An individual is prompted by the following screen when attempting to connect her bank account:

[4] *Id.*

Figure 1



46. The first screen displayed in Figure 4 states that "[PayPal] use[s] Yodlee to confirm your bank details and to check your balance and transaction as needed, which can help your PayPal payments go through." This limited interaction is all that the individual consents to. Nowhere does she give either PayPal or Envestnet | Yodlee permission to collect and store data for resale.

47. Yet if a user uses Envestnet | Yodlee to link their bank account to PayPal, Envestnet | Yodlee will harvest a copy of the user's login credentials for its own purposes that far exceed the disclosed scope in at least three ways. *First*, Yodlee will use those credentials without any regard for what is "needed" to "help [the user's] Paypal payments go through." Rather, they will acquire massive quantities of data for their own purposes. *Second*, by Envestnet | Yodlee's own admission, Yodlee immediately obtains 90 days' worth of transaction information once a user links an account—even though those 90 days of transactions are unrelated to the single transaction for which consumers linked their banking institution with PayPal. Yodlee then retains the usernames and passwords to "refresh" individuals' account information on an ongoing, daily basis, whether or not the individual uses PayPal on a given day. Indeed, even if the user never uses PayPal again,

Envestnet | Yodlee continues to collect data from their accounts on an ongoing basis. *Third*, Yodlee then sells this data as part of large compilations of individual transactions that remain traceable to particular individuals. Nowhere does the user give either PayPal or Yodlee permission to do any of this.

48. The second screen displayed in Figure 4 is also misleading. This screen informs consumers that, "[y]ou can choose which eligible bank accounts from WELLS FARGO you want to link to Paypal." This communicates to consumers that only chosen accounts, a subset of their banking information, will be accessed. This is false. In truth, after acquiring a user's credentials by linking even a single account, Envestnet | Yodlee repeatedly accesses *all* activity and *all* accounts connected to those credentials.

49. The individual never consents to this kind of data collection, which solely benefits Yodlee.

50. An individual cannot opt out of or turn off Envestnet | Yodlee's access to her bank account information after providing her credentials. For example, while the first screen in Figure 4 states, "[y]ou can turn off our use of Yodlee by removing permissions for this Bank in your Profile," this pertains only to PayPal's access to user data. Envestnet | Yodlee still retains the individual's credentials and continues to access her bank account to collect and sell highly sensitive financial data without consent even after PayPal's permissions to that data are removed.

51. Envestnet | Yodlee's recurring collection of and continued access to an individual's financial data is never disclosed. Envestnet | Yodlee's privacy policy only applies to its own direct-to-consumer products and does not cover the APIs that power FinTech Apps or facilitate log in transactions like that described in Figure 4.[5] Instead, Envestnet | Yodlee directs an individual using "Yodlee powered services delivered through a Yodlee client" such as PayPal to refer to the "client's data governance and privacy practices." Thus, where an individual unknowingly uses Envestnet |

[5] Yodlee, Inc., *Privacy Notice* (last updated July 31, 2020), https://www.yodlee.com/legal/privacy-notice.

Yodlee to connect her bank accounts to a FinTech App, there is nowhere she could have looked in Envestnet | Yodlee's policies to learn the full extent of data Yodlee was collecting from her or the fact that Yodlee was selling her data.

52. Nor does Envestnet | Yodlee require its FinTech App clients to make any such disclosures. For example, while the PayPal Privacy Statement linked to in the first screen of Figure 4 discloses that PayPal does not "sell [individuals'] personal data," it says nothing about whether service providers, such as Envestnet | Yodlee, collect and sell such sensitive financial data. Likewise, while the PayPal Privacy Statement provides that "you *may* be able to manage how your personal data is collected, used, and shared by [third-parties]," it does not provide individuals with a way to manage what data Yodlee collects about them through PayPal or how Yodlee uses and shares that data with others. Such controls would have to come directly from Envestnet | Yodlee, which does not allow individuals to manage their personal data, because doing so would undermine Yodlee's highly profitable data business.

53. Not only does Yodlee collect more data than is necessary from individuals that interact with their FinTech Apps—Yodlee's service is not necessary at all.

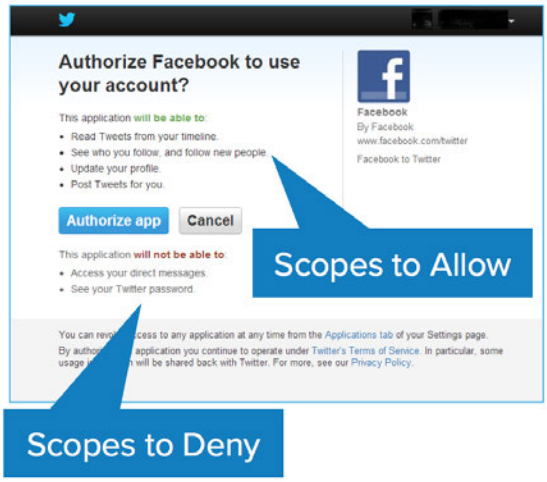
54. Historically, in order to allow a third party access to a bank account, a user had to submit her bank routing and account numbers; transfer a small trial deposit (usually a few cents); and then return to the bank to verify the amount transferred. This process usually took several days, a delay that could—in the fast-moving Internet age—cause potential users of FinTech Apps to give up on using the app at all.

55. One alternative to this process is "OAuth." Users are likely familiar with this procedure because it has become the industry-standard protocol for users who wish to grant a website or an app permission to access certain information from another website or app. Crucially, OAuth "enables apps to obtain limited access (scopes) to a user's data without giving away a user's password."[6] For instance, consider an example in which a user wishes to grant Facebook permission

[6] *See* Matt Raible, *What the Heck is Oauth?* OKTA (June 21, 2017), https://developer.okta.com /blog/2017/06/21/what-the-heck-is-oauth..

to access her Twitter account so that it can integrate its social media accounts together. Before it can do so, the user will be redirected from Facebook to Twitter, where it must login to ensure it is authorized to grant those permissions.[7] Then, a dialogue box pops up, asking which permissions the user is granting and which it is denying. The dialogue box might look something like this:[8]

Figure 2



56. In this example, note that the user grants Facebook permission to update her Twitter profile and even post to the user's Twitter account ("This application will be able to . . . Update your profile; Post Tweets for you"), but *denies* Facebook permission to see the user's Twitter password ("This application will not be able to . . . See your Twitter password"). Instead, the user provides her Twitter username and password only to Twitter. Twitter then sends a "token" to Facebook, essentially confirming to Facebook that the user's login to Twitter was legitimate. Scopes are one of the "central components" and perhaps even "the first key aspect" of OAuth.

57. But as with the old-fashioned way of authorizing a bank account by providing account and routing numbers and waiting for a small deposit, OAuth requires a user to leave the app and be redirected to another site or interface to log in. This supposedly undermines an app's ability to sign up new users by driving away individuals who decide it is not worth the trouble of

---

[7] Redirection from the app the user is currently using to the app where it retains the data to which it is granting permission is a hallmark of OAuth.

[8] Raible, *supra* n.6.

dealing with the OAuth process.

58. Envestnet | Yodlee's API purports to solve this problem, but the distinctions between Envestnet | Yodlee's API and true OAuth underscore the grave risk that Envestnet | Yodlee poses to individuals. *First*, Envestnet | Yodlee does not provide a clear dialogue box outlining the scopes of the permissions that the user is granting to Envestnet | Yodlee or the permissions the user is denying to Envestnet | Yodlee. Indeed, the user has no option to deny Envestnet | Yodlee any permissions at all.

59. *Second*, the core principle of OAuth—and what has made it the industry-standard authorization protocol—is that it provides for access to an individual's data *without disclosing the individual's password* to the service requesting authorization. This places the individual in control because she can cut off the service's access to her data by revoking the service's OAuth access. Envestnet | Yodlee specifically designed its API to circumvent this protection, deceiving users into providing Yodlee with their bank usernames and passwords so that Yodlee can use those credentials to collect sensitive financial information on an ongoing basis without giving the individual a way to revoke access to that data. As explained above, Yodlee accomplishes this by deceiving users into thinking that they are logging into their financial institutions' app or website, when in fact they are entering their credentials directly into Yodlee's portal.

60. Envestnet | Yodlee is capable of integrating OAuth into its API. It has done so in Europe to comply with the European Union's Second Payment Services Directive. Yet in the United States, Yodlee continues to deploy credential-based authentication because, though it falls short of the industry standard, it is a source of immense profit.

61. By failing to provide disclosures or obtain users' consent to collect and sell their sensitive personal data, Yodlee violated Plaintiffs' and Class members' privacy rights and state and federal law.

III. ENVESTNET | YODLEE STORES CONSUMERS' DATA FOR BACKUP PURPOSES

62. As noted above, once a consumer uses the Envestnet | Yodlee API to link her financial account to a FinTech app, Envestnet | Yodlee receives the credentials for the user, generates a unique identifier, and opens a profile for that user. Envestnet | Yodlee then immediately harvests 90 days' worth of transactional data from all of that user's accounts and continues to extract user data going forward. Envestnet | Yodlee then adds the data to that user's profile.

63. Envestnet | Yodlee provides this data to developers who incorporate the Envestnet | Yodlee API into their FinTech apps. Developers are able to store this information on their own databases and perform analytics as necessary for their FinTech apps to function.

64. Envestnet | Yodlee stores a copy of consumers' data for backup purposes on behalf of developers. For example, if a developer loses access to the data, it can download the data again from Envestnet | Yodlee's servers.

65. Envestnet | Yodlee also stores a copy of consumers' financial transaction data for its own backup purposes. As Envestnet | Yodlee reported in its prospectus prior to the proposed merger with Envestnet, the company "has formal disaster recovery programs for Yodlee's internal services and Yodlee's customers' applications. . . . In addition, Yodlee's infrastructure consists of highly redundant environments. This includes redundant equipment at every layer with various configurations such as active/active and active/failover. . . . [T]he Company and each of its Subsidiaries has implemented and maintains commercially reasonable security, backup and disaster recovery policies, procedures and systems designed to reasonably maintain the security and operation of the respective businesses of the Company and each of its Subsidiaries."[9] Envestnet likewise discloses that "[i]n the event of an internal or external [significant business disruption] that causes the loss of our paper records, we will access electronic versions of these records in our various systems and platforms. If our primary site is inoperable, we will continue operations from our backup site or an alternate location. For the loss of electronic records, we will recover the

[9] Yodlee, Inc., Proxy Statement/Prospectus, (October 14, 2015), https://www.sec.gov/Archives/edgar/data/1337619/000104746915007906/a2226277z424b3.htm.

electronic data from our backup records stored in the disaster recovery site, or, if our primary site is inoperable, continue operations from our backup site."[10]

66. On information and belief, the data described in these disclosures include Plaintiffs' and Class members' financial transaction data.

67. Envestnet | Yodlee reserves Plaintiffs' and Class members' financial transaction data for future use, or in the event that it needs to be transmitted again.

68. While in electronic storage, Envestnet | Yodlee divulges Plaintiffs and Class members' financial transaction data to its clients.

IV. ENVESTNET | YODLEE'S FAILURE TO DISCLOSE VIOLATES SEVERAL PRIVACY LAWS

69. As discussed above, Envestnet | Yodlee's privacy policy only applies to its "direct-to-consumer services and websites." For consumers who access Envestnet | Yodlee's services through one of Envestnet | Yodlee's clients, such as PayPal, Envestnet | Yodlee pushes off the burden of providing adequate disclosures to consumers onto the client.

70. This is an abdication of Yodlee's duties under the law.

71. In California, several statutes require Yodlee to provide clear disclosures to consumers about their conduct, including that they collect and sell consumers' sensitive personal data.

72. For example, the California Consumer Privacy Act ("CCPA") protects consumers' personal information from collection and use by businesses without providing proper notice and obtaining consent.

73. The CCPA applies to Yodlee because it earns more than $25 million in annual gross revenue. Additionally, the CCPA applies to Yodlee because it buys, sells, receives, or shares, for commercial purposes, the personal information of more than 50,000 consumers, households, or devices.

74. The CCPA requires a business that collects consumers' personal information, such

[10] Envestnet, Inc., *Business Continuity*, (June 19, 2020), https://www.envestnet.com/business-continuity.

as Yodlee, to disclose either "at or before the point of collection . . . the categories of personal information to be collected and the purposes for which the categories of personal information shall be used." Cal. Civ. Code § 1798.100(b).

75. Furthermore, "[a] business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section." *Id.*

76. Other state statutes that govern Yodlee's disclosures include California's Financial Information Privacy Act ("CalFIPA"), Cal. Fin. Code § 4053(d)(1), and the California Online Privacy Protection Act ("CalOPPA"), Cal. Bus. & Prof. Code § 22575. CalFIPA requires that the language in privacy policies be "designed to call attention to the nature and significance of the information" therein, use "short explanatory sentences," and "avoid[] explanations that are imprecise or readily subject to different interpretations." Cal. Fin. Code § 4053(d)(1). The text must be no smaller than 10-point type and "use[] boldface or italics for key words." *Id.* In passing CalFIPA, the California legislature explicitly provided that its intent was "to afford persons greater privacy protections than those provided in . . . the federal Gramm-Leach-Bliley Act, and that this division be interpreted to be consistent with that purpose." Cal. Fin. Code § 4051. *See infra*.

77. CalOPPA requires that an operator of any online service, as defined therein, "conspicuously post" its privacy policy. Cal. Bus. & Prof. Code § 22575. Under the statute, to "conspicuously post" a privacy policy via a text hyperlink, the hyperlink must include the word "privacy," be "written in capital letters equal to or greater in size than the surrounding text," or be "written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language." Cal. Bus. Prof. Code § 22577(b).

78. The Graham Leach Bliley Act (the "GLBA") and the regulations promulgated thereunder impose strict requirements on financial institutions regarding their treatment of consumers' private financial data and the disclosure of their policies regarding the same. Yodlee is a financial institution subject to those regulations, which include the Privacy of Consumer Financial Information regulations (the "Privacy Rule"), 16 C.F.R. Part 313, re-codified at 12 C.F.R. Part 1016

("Reg. P"), and issued pursuant to the GLBA, 15 U.S.C. §§ 6801-6803, and the GLBA's "Safeguards Rule" (16 C.F.R. Part 314).

79. This regulatory scheme has clear requirements for applicable privacy policies. Under those rules, a financial institution "must provide a clear and conspicuous notice that accurately reflects [its] privacy policies and practices." 16 C.F.R. § 313.4. Privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). Ways a company can call attention to its privacy policy include "[using] a plain-language heading" (16 C.F.R. § 313.3(b)(2)(ii)(A); "[using] a typeface and type size that are easy to read" (16 C.F.R.§ 313.3(b)(2)(ii)(B)); (c) "[using] boldface or italics for key words" (16 C.F.R. § 313.3(b)(2)(ii)(D)); or (d) "[using] distinctive type size, style, and graphic devices, such as shading or sidebars," when combining its notice with other information (16 C.F.R. § 313.3(b)(2)(ii)(E)). A company must ensure that "other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice." 16 CFR § 313(b)(2)(iii). The notice should appear in a place that users "frequently access." 16 CFR § 313.3(b)(2)(iii)(A), (B). Privacy notices must "accurately reflect[]" the financial institution's privacy policies and practices. 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. The notices must include the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies. 16 C.F.R.§ 313.6; 12 C.F.R. § 1016.6.

80. Both GLBA and CalFIPA require that privacy policies provide consumers with an opportunity to opt out of the sharing of their personal data. 16 C.F.R. § 313.10; Cal. Fin. Code. § 4053(d)(2).

81. Yodlee violated these statutory and regulatory requirements because it does not disclose through the Envestnet | Yodlee privacy policy that it collects consumers' personal information, let alone the categories of personal information it collects, nor the purposes for which

this information is collected.

82. Envestnet | Yodlee's privacy policy is not "clear and conspicuous." Worse still, Envestnet | Yodlee *does not even maintain* a privacy policy that applies to users of third party Fintech Apps, such as Plaintiffs and Class members here. Envestnet | Yodlee's privacy policy applies only to users of its direct-to-consumer apps and does not cover the unauthorized data collection practices alleged throughout this Complaint.

83. Nor does Envestnet | Yodlee make these necessary disclosures at the "point of collection." For example, as discussed above, when consumers connect their bank account to PayPal through Envestnet | Yodlee, nowhere is it disclosed that Envestnet | Yodlee collects and sells consumers' sensitive personal data. All that is disclosed is that "[PayPal] use[s] Yodlee to confirm your bank details and to check your balance and transaction as needed, which can help your PayPal payments go through." This is materially false and misleading in that it does not disclose: (1) that Envestnet | Yodlee collects and sells users' sensitive personal data; (2) the categories of data that Envestnet | Yodlee collects and sells; or (3) the true purpose for Envestnet | Yodlee's conduct, i.e., to earn monetary compensation by selling Plaintiffs' and Class members' data to other entities. Other apps that incorporate Envestnet | Yodlee's API, such as Personal Capital, do not disclose their use of Envestnet | Yodlee in the screens that consumers see while using the app.

84. Further, Envestnet | Yodlee's privacy policy provides an insufficient opportunity to opt out, including because it fails to use the heading "Restrict Information Sharing With Other Companies We Do Business With To Provide Financial Products And Services." Cal. Fin. Code § 4053 (d)(1)(A).

85. In addition to being financial institutions themselves, governed by the GLBA and CalFIPA, Yodlee also received data from other financial institutions. As such, they violated the following CalFIPA provision as well:

> **An entity that receives nonpublic personal information pursuant to any exception set forth in Section 4056 shall not use or disclose the information except in the ordinary course of business** to carry out the activity covered by the exception under which the information was received.

Cal. Fin. Code § 4053.5 (emphasis added).

86. One of the exceptions noted in Section 4056 allows sharing of nonpublic personal information "with the consent or at the direction of the consumer." Cal. Fin. Code. § 4056. Plaintiffs and Class members did not consent to or direct the release of their sensitive nonpublic personal information for the reasons described herein. But even if they did, Section 4053.5 still provides that an entity like Envestnet | Yodlee can *only* use such information to carry out the activity *for which the user provided consent*. Yodlee's use of the data for any reason other than connecting users' bank accounts violates this statutory protection.

V. GOVERNMENT AND INDUSTRY LEADERS AGREE THAT YODLEE'S CONDUCT IS WRONG, RISKY, DANGEROUS AND BAD FOR CONSUMERS

87. Government and industry leaders agree that Yodlee's conduct runs afoul of basic standards of decency and proper treatment of consumer data.

88. The Consumer Financial Protection Bureau's ("CFPB") 2017 Consumer Protection Principles for data harvesters like Envestnet | Yodlee provide that such services should not "require consumers to share their account credentials with third parties"—i.e., anyone other than the user or the bank.[11] Of course, Yodlee does exactly that.

89. Likewise, the Consumer Protection Principles provide that the data practices of a company like Envestnet | Yodlee must be, "fully and effectively disclosed to the consumer, understood by the consumer, not overly broad, and consistent with the consumer's reasonable expectations in light of the product(s) or service(s) selected by the consumer." Yodlee's disclosures were not full and effective, as described above. Yodlee's data practices were likely to and did deceive Plaintiffs and Class members, are overly broad, and are not consistent with consumers'

---

[11] CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

reasonable expectations, because they are out of proportion with what is necessary to link financial accounts to FinTech apps.

90. The Consumer Protection Principles also provide that data access terms must address "access frequency, data scope, and retention period." Nowhere does Yodlee disclose how it accesses consumers' data, how much data it gathers, and how long is keeps it—perhaps because consumers would be outraged to hear the answers.

91. The Consumer Protection Principles also provide that consumers must be informed of any third parties that access or use their information, including the "identity and security of each such party, the data they access, their use of such data, and the frequency at which they access the data." Yodlee does not disclose this information.

92. The CFPB recently issued an advance notice of proposed rulemaking ("ANPR") to address the abuses and increasing privacy concerns stemming from the conduct of data harvesters like Envestnet | Yodlee.[12] The ANPR is evidence of increasing government and agency concern over the numerous ways in which practices like Envestnet | Yodlee's harm millions of consumers.

93. Major financial institutions and their trade associations have also voiced concerns. In April 2016, J.P. Morgan CEO Jamie Dimon said the bank is "extremely concerned" about "outside parties," including "aggregators" (like Yodlee), for three reasons: first, "[f]ar more information is taken than the third party needs in order to do its job"; second, "[m]any third parties sell or trade information in a way [users] may not understand, and the third parties, quite often, are doing it for their own economic benefit – not for the customer's benefit"; and third, "[o]ften this is being done on a daily basis for years after the customer signed up for the services, which they may no longer be using."[13] Dimon recommended that users not share their login credentials with third

---

[12] CFPB, *Consumer Financial Protection Bureau Releases Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records*, (October 22, 2020), https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-releases-advance-notice-proposed-rulemaking-consumer-access-financial-records/.

[13] *See* Jamie Dimon, Chairman and CEO of JPMorgan Chase & Co., Letter to Shareholders, (Apr. 6, 2016), https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/2015-annualreport.pdf.

parties like Envestnet | Yodlee, in part to avoid loss of important indemnification rights: "When [users] give out their bank passcode, they may not realize that if a rogue employee at an aggregator uses this passcode to steal money from the customer's account, the customer, not the bank, is responsible for any loss. . . . This lack of clarity and transparency isn't fair or right." J.P. Morgan hit the nail on the head in identifying the egregious invasions of privacy that are not simply incidental to Yodlee's business, but lie at the heart of it.

94. Envestnet | Yodlee admits that major financial institutions have expressed security concerns about its practices. In 2017, the company said that "several large banks had told it that it would lose access to at least some data in the near future if it did not agree to new restrictions on the data it is pulling."[14] That same year, Jason Kratovil, the vice president for government affairs for payments at the Financial Services Roundtable, a trade association for banks, said, "[w]hen you think about millions of customers handing over their bank-account credentials to third parties, who currently have no real oversight or examination of their security controls, you start to understand why our members get pretty nervous."[15]

95. In 2017, the American Bankers Association ("ABA") wrote to the CFPB to express similar concerns.[16] The ABA stated that "few consumers appreciate the risks presented when they provide access to financial account data to non-bank fintech companies," including the risk of removing such data from the secure bank environment; that "consumers are not given adequate information or control over what information is being taken, how long it is accessible, and how it will be used in the future"; that companies like Envestnet | Yodlee make "little effort to inform consumers about the information being taken, how it is being used or shared, how often it is being

---

[14] Nathaniel Popper, *Banks and Tech Firms Battle Over Something Akin to Gold: Your Data*, N.Y. Times (March 23, 2017), https://www.nytimes.com/2017/03/23/business/dealbook/banks-and-tech-firms-battle-over-something-akin-to-gold-your-data.html

[15] *Id.*

[16] Rob Morgan, Vice President, Emerging Technologies of American Bankers Association, Letter Response to Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048 (Feb. 21, 2017), https://www.aba.com/-/media/documents/comment-letter/aba-comment-cfpb-data-aggregators.pdf?rev=a5603ffb382c49059ebab1dfda631abf.

accessed, and how long the aggregator will continue to access it"; and that "[c]onsumers assume that data aggregators take only the data needed to provide the service requested," but in reality, "too often it is not the case."

VI. PLAINTIFFS AND CLASS MEMBERS LOST INDEMNIFICATION RIGHTS AND OTHER RIGHTS AND PROTECTIONS

96. Under federal regulations, a consumer is not liable for unauthorized electronic fund transfers from her financial accounts, subject to certain limits and conditions. *See, e.g.*, 12 C.F.R. § 1005.2(m). But Yodlee's conduct eliminates consumers' rights to indemnification under these regulations. If Yodlee induced Plaintiffs and Class members to provide their bank credentials to Yodlee, and a malicious user subsequently uses those credentials to access and improperly transfer funds from Plaintiffs and Class members' accounts, banks consider that transfer to have been authorized because of the initial provision of the credentials to Yodlee. As noted above, J.P. Morgan CEO Jamie Dimon expressed concern that consumers do not generally understand that they will be responsible for any such loss. For instance, a theft of $10,000 from a consumer's account would ordinarily leave a consumer liable for only $50; but if Yodlee's conduct in any way contributes to that unlawful access, the consumer may now be liable for the full $10,000, a loss in value of $9,950.

97. In 2019, J.P. Morgan Chase acted on these concerns by entering an agreement with Envestnet | Yodlee to prohibit Yodlee from harvesting Chase customers' banking credentials. The agreement specified that users' data would no longer be transmitted via Envestnet | Yodlee's unsecure API. Instead, the data would be transmitted to Envestnet | Yodlee via JPM's own custom, secure API. Chase's head of digital banking stated that the change "will help our customers manage exactly who they give their information to, and understand how their information will be used."[17] The press release stated, "[b]ecause the secure API uses a token-based approach, customers will no longer need to give out their username and password – confidential credentials that should always be treated with the utmost care." Other banks such as Bank of America, Citi and Wells Fargo have

[17] Business Wire, *JPMorgan Chase, Envestnet Yodlee Sign Agreement to Increase Customers' Control of Their Data* (December 5, 2019), https://www.businesswire.com/news/home/20191205005462/en/JPMorgan-Chase-Envestnet-l-Yodlee-Sign-Agreement-to-Increase-Customers%E2%80%99-Control-of-Their-Data.

taken similar action.

98. By removing Plaintiffs' and Class members' data from their bank's secure environment and storing it in Yodlee's own computer systems, networks or servers, Yodlee has destroyed the rights and protections to which Plaintiffs and Class members are otherwise entitled. That amounts to an economic loss to Plaintiffs and Class members.

99. Even if a particular Plaintiff's or Class member's account has not been compromised, the indemnification and related rights are vested rights that Plaintiffs and Class members are entitled to assert against their bank in the event their data is misused. Those rights are lost as soon as Envestnet | Yodlee remove Plaintiffs' and Class members' data from their bank's secure environment, as the bank is no longer in control of (and thus responsible for) what happens to that data. Just as a person derives a benefit from having an insurance policy in place and loses that benefit if he is deprived of that policy—regardless of whether he has made a claim against that policy—Plaintiffs' and Class members' loss of indemnification rights and related rights and protections occurs even if they have not sought to enforce them. Plaintiffs' and Class members' loss of indemnification rights and related rights and protections amounts to cognizable and measurable economic damage and loss of money and property.

VII. PLAINTIFFS AND CLASS MEMBERS LOST CONTROL OVER VALUABLE PROPERTY AND THE ABILITY TO RECEIVE COMPENSATION FOR IT

100. The data that Yodlee collects, retains and sells has enormous value both to Yodlee and to the Plaintiffs and Class members from whom Yodlee illicitly obtains it.

101. First, the data at issue is valuable to Yodlee. The market for consumer data is worth as much as $200 billion.[18] In 2015, Envestnet announced an acquisition of Yodlee for $590 million, based in large part on the universe of consumer data that Yodlee had accumulated. Yodlee packages and sells the data it collects to third party customers, thus demonstrating that there is an active market for Plaintiffs' and Class members' data. The sheer size of this mountain of data, as well as Yodlee's ability to continue accessing Plaintiffs' and Class members' transaction histories on an

[18] Catherine Tucker, *Buying Consumer Data? Tread Carefully*, Harvard Business Review, (May 1, 2020), https://hbr.org/2020/05/buying-consumer-data-tread-carefully.

ongoing basis, creates a competitive advantage that Yodlee may exercise over their competitors. Once Yodlee acquires the data, however, Plaintiffs and Class members have no control over what Yodlee does with it, including how it packages it and to whom it sells it.

102. The data at issue is also valuable to Plaintiffs and Class members, but Yodlee's conduct has impeded the possibility of a robust and equitable market for consumer data emerging in which Plaintiffs and Class members would be compensated for it.

103. Marketplaces exist in which data brokers purchase consumers' data from them. For instance, Brave is a web browser that allows consumers to surf the internet free of surveillance (unlike some other browsers), while offering the option to allow Brave to observe their activity and collect data in exchange for basic attention token ("BAT"), a currency that can be traded for approximately one dollar per BAT.

104. Brave estimated in 2019 that users would be able to earn between $60 and $70 that year—and possibly over $200 in 2020—by selling access to their data through the Brave software.[19] There is currently over $1 billion in BAT outstanding, with as much as $54 million worth of the currency traded per day.[20]

105. Brave states that its mission is to allow users to "take back control" and to stop "data harvesters [which] are . . . granted access to your personal identity and online habits so that they can make billions in annual profits."[21] Brave garnered 20 million users in 2020, which shows that consumers have substantial interest in receiving compensation for their data.

106. In the context of consumer financial data, no such market presently exists. A company called Datacoup paid consumers as much as $8 per month for access to, among other things, their credit card transaction data. But Datacoup dissolved because it could not achieve the same scale as companies like Envestnet | Yodlee, which harvests data from millions of consumers

---

[19] Michael Kan, *Brave Browser Will Pay You to View Ads (But There's a Catch)*, PC Magazine, (Jan. 15, 2019), https://www.pcmag.com/news/brave-browser-will-pay-you-to-view-ads-but-theres-a-catch.

[20] Coincap.io Data Market Website (last visited March 14, 2021), https://coincap.io/.

[21] *Get Rewarded for Paying Attention*, Brave, (Mar. 11, 2021) https://brave.com/compare/chrome/earning/.

without paying them. As *Forbes* reported at the time, "The problem for such new companies is that marketers will not pay much for details about just thousands of people when data brokers who pay nothing to individuals offer detailed dossiers on millions."[22]

107. Such a market would allow Plaintiffs and Class members to retain agency, control and power over their intimate information, and receive compensation in exchange for knowingly and willingly turning it over. But any hope of such a market emerging has only become less likely in the face of Yodlee's abusive practices. Envestnet | Yodlee's stockpile of consumer financial data and the user credentials it deploys to constantly refresh that data operate as a barrier to entry by any new competitors. Any new entrant who planned to pay users for the same type of data that Envestnet | Yodlee takes would face an extraordinary task of accumulating sufficient data to support a viable business. Instead, Yodlee dominates a multi-billion-dollar market in which they alone derive economic benefit from consumers' private, highly sensitive, and valuable data.

108. Yodlee's conduct is a substantial factor inhibiting the development of a market for Plaintiffs and Class members to sell access to their data. Envestnet | Yodlee has thus deprived consumers of the value of their data by impeding such markets from developing. This amounts to an economic loss of money and property for Plaintiffs and Class members.

VIII. PLAINTIFFS AND CLASS MEMBERS SUFFERED AN INCREASED RISK OF IDENTITY THEFT AND FRAUD

109. Yodlee's conduct increases the likelihood that Plaintiffs' and Class members' accounts will be compromised. As the ABA recognizes, the "sheer volume and value of the aggregated data" warehoused at entities like Yodlee makes them "a priority target for criminals, including identity thieves." Databases like Yodlee's create a one-stop shop for malicious actors to gain access to all of a consumer's accounts, creating a "rich reward for a single hack." Yodlee's consolidation of risk to consumers at a single point of entry creates tangible, economic injury to Plaintiffs and Class members, who must spend time and money closely monitoring their credit reports and other financial records for any evidence that their accounts have been compromised.

[22] Adam Tanner, *Others Take Your Data for Free, This Site Pays Cash*, Forbes Magazine, (March 3, 2019), https://www.forbes.com/sites/adamtanner/2014/03/03/others-take-your-data-for-free-this-site-pays-cash/?sh=5c62f4679461.

Plaintiffs and Class members face an expanded and imminent risk of economic harm from unauthorized transfers, identity theft, and fraud.

110. Given the secret, undisclosed nature of Yodlee's data collection practices, Plaintiffs anticipate that discovery and expert analysis are likely to demonstrate additional types of economic loss or damage and/or damage to money and property and reserve their rights to amend this Complaint to assert those theories at the appropriate time.

IX. PLAINTIFFS AND CLASS MEMBERS HAVE A REASONABLE EXPECTATION OF PRIVACY

111. Plaintiffs' and Class members' expectation of privacy in their highly sensitive personal data, which Yodlee collected, sold, or otherwise misused, is enshrined in California's Constitution. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy*." Art. I., Sec. 1, Cal. Const. (emphasis added).

112. The phrase "*and privacy*" was added in 1972 after a proposed legislative constitutional amendment designated as Proposition 11. Significantly, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating in relevant part:

> **The right of privacy is the right to be left alone.** It is a fundamental and compelling interest. It protects **our homes**, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose. **It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us.**
>
> **Fundamental to our privacy is the ability to control circulation of personal information.** This is essential to social relationships and personal freedom. The proliferation of government and business records over which we have no control limits our ability to control our

> personal lives. Often we do not know that these records even exist and we are certainly unable to determine who has access to them.[23]

113. Consistent with the language of Proposition 11, numerous studies examining the collection of consumers' personal data confirm that the surreptitious taking of personal, confidential, and private information from millions of individuals, as Envestnet | Yodlee has done here, violates expectations of privacy that have been established as general social norms.

114. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its users' personal data.

115. For example, a recent study by *Consumer Reports* shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing their data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them. Moreover, according to a study by *Pew Research*, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.

116. Yodlee failed to disclose that they collected, sold, and otherwise misused consumers' sensitive personal data, and failed to obtain consent to do so. This constitutes a violation of Plaintiffs' and Class members' privacy interests, including those enshrined in the California Constitution.

X. YODLEE LACKS ADEQUATE SAFEGUARDS TO PROTECT CONSUMERS' DATA

117. When Envestnet | Yodlee sells Plaintiffs and Class members' data, it claims to sell it only in "aggregated" form, with all information "de-identified." But in fact, Yodlee's Data and Analytics products consist of bulk records of individual transactions, or what Envestnet itself has called "aggregated transaction-level account data elements."[24] Thus, even though Yodlee's data products may be "aggregated" in the sense that they contain data from thousands or millions of

---

[23] Ballot Pamp., Proposed Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972) at 27 (emphasis added).

[24] Envestnet, Inc., Form 10-k at 8, (December 31, 2020), https://sec.report/Document/0001628280-21-003457/.

individual consumers, they still contain details about individual transactions. Third party purchasers receive more than enough information to re-identify particular individuals from the data set.

118. Envestnet | Yodlee claims that "[p]rotecting the personal information of those who use our services is [their] top priority," and that it employs, "leading industry standards of de-identification processing," and "technical, administrative, and contractual measures to protect consumers' identities, such as prohibiting analytics and insights users from attempting to re-identify any consumers from the data."[25] These statements are false.

119. According to leaked documents obtained by *Vice News*, Envestnet | Yodlee's data anonymization process involves "removing names, email addresses, and other personally identifiable information (PII) from the transaction data."[26] This includes "masking patterns of numbers such as account numbers, phone numbers, and SSNs and replacing them with 'XXX' symbols" and "mask[ing] the financial institution's name in the transaction description."[27]

120. However, Envestnet | Yodlee's customers (and potential identity thieves) still receive a wealth of information that can be used to re-identify an individual. For example, even Envestnet | Yodlee's "masked" information still provides a unique identifier for who made the purchase, the amount of the transaction, date of sale, the city, state and zip code of the business where the purchase was made, and primary and secondary merchant fields, that can be combined to identify the specific individual involved in each transaction.

121. Moreover, because Envestnet | Yodlee keeps a unique identifier for each individual consumer in its data set, and these identifiers are preserved across all transactions, marketers (and cybercriminals) can de-anonymize the data by linking multiple transactions by the same user and combining that information with other publicly available data.

122. As Yves-Alexandre de Montjoye, an associate professor at Imperial College London explained, this data is more "pseudonymized" than anonymized, meaning that while "it doesn't

---

[25] *See* Vice (Joseph Cox), *supra* n. 3.

[26] *Id.*

[27] *Id.*

contain information that'd directly identify a person such as names or email addresses . . . someone with access to the dataset and some information about you . . . might be able to identify you."

123. Vivek Singh, an associate professor at Rutgers University, raised the same concern, because the data "does not remove spatio-temporal traces of people that can be used to connect back the data to them." Spatio-temporal traces are data associated with the transaction, including the date, merchant, and physical location.

124. Singh and de Montjoye authored a 2015 study published in *Science* in which they successfully identified individuals using a dataset of similar "de-identified" data with just three months of transactions—the amount of data Envestnet | Yodlee initially collects from Class members—covering 1.1 million people.[28] Singh explained with just "three to four" transactions, an attacker "can unmask the person with a very high probability." The study concluded that it was possible to determine the identity of an individual from so-called "anonymized" credit card data 90% of the time through simple extrapolation.[29]

125. Significantly, last year, scientists from the Imperial College London and Université Catholique de Louvain reported that they have developed a model that can re-identify 99.98% of Americans from datasets using as few as fifteen demographic attributes. Notably, these researchers have made their software code available for anyone on the internet.

126. Consumers whose information is collected and sold by Envestnet | Yodlee are especially vulnerable because a user's credit and debit card transactions can reveal a wealth of other personal and demographic information, such as health, sexuality, religion, and political views that can be used to re-identify individuals like Plaintiffs and Class members.

127. These studies confirm that Envestnet | Yodlee's purported "deanonymization" provides little to no protection for Plaintiffs and Class members, given the immense amount of data that Envestnet | Yodlee has been able to collect through its network of over 17,000 connections to

---

[28] Y. de Montjoye, V. Singh et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 357 Science 6221, 536-539 (Jan. 30, 2015), https://science.sciencemag.org/content/347/6221/536?mod=article_inline.

[29] *Id.*

financial institutions, billers, reward networks, and other endpoints.

128. Furthermore, despite Envestnet | Yodlee's claim that it employs "technical, administrative, and contractual measures to protect consumers' identities, such as prohibiting analytics and insights users from attempting to re-identify any consumers from the data,"[30] Yodlee does not have reasonable safeguards in place to protect consumers' sensitive personal data.

129. Envestnet | Yodlee admitted in a 2015 filing with the SEC that it "does not audit its customers to ensure that they have acted, and continue to act, consistently with such assurances."[31] After selling consumer data, Yodlee takes no steps to ensure this information remains private, that their clients are not attempting to re-identify consumers, or use that data for malicious purposes.

130. Nor could they. Envestnet | Yodlee's choice not to employ technical safeguards to protect consumers' sensitive personal data and instead to sell that data to their clients in large text files removes their ability to exert any control over the information once it has been sold.

131. In 2015, Envestnet | Yodlee hired Peter Swire, a professor of law and ethics at Georgia Institute of Technology and former Obama administration official, to review its privacy practices after receiving questions from the Wall Street Journal. Swire told the Journal that Envestnet | Yodlee is "doing the technical and administrative things that regulators have recommended" to make sure consumers remain anonymous. Professor Swire also provided a comment for Envestnet | Yodlee's website, opining that Professors Singh and de Montjoye's findings "do not apply to the Yodlee facts."[32] But that statement no longer appears on the Envestnet | Yodlee website. And in 2020, when a reporter asked Swire if he stood by his statements from 2015, he said only, "I have no comment."[33]

---

[30] *See* Vice (Joseph Cox), *supra* n. 3.

[31] Yodlee, Inc., Proxy Statement/Prospectus, *supra* n. 9.

[32] *See* Vice (Joseph Cox), *supra* n.3.

[33] *Id.*

XI. MEMBERS OF CONGRESS REQUESTED AN FTC INVESTIGATION INTO YODLEE'S PRACTICES

132. Last year, three members of Congress wrote a letter urging the FTC to investigate Yodlee for selling Americans' highly sensitive data without their knowledge or consent.[34]

133. In the letter, Senator Ron Wyden, Senator Sherrod Brown, and Representative Anna Eshoo wrote that "Envestnet [] sells access to consumer data . . . The consumer data that Envestnet collects and sells is highly sensitive. Consumers' credit and debit card transactions can reveal information about their health, sexuality, religion, political views, and many other personal details . . . And the more often that consumers' personal information is bought and sold, the greater the risk that it could be the subject of a data breach."[35]

134. The three members of Congress were deeply worried that "Envestnet and the companies to which it had sold data [did not] have the required technical controls in place to protect Americans' sensitive financial data from re-identification, unauthorized disclosure to hackers or foreign spies, or other abusive data practices." [36]

135. The letter further warned that:

> Envestnet does not inform consumers that it is collecting and selling their personal financial data . . . Instead, Envestnet only asks its partners, such as banks, to disclose this information to consumers in their terms and conditions or privacy policy. That is not sufficient protection for users. Envestnet does not appear to take any steps to ensure that its partners actually provide consumers with such notice. And even if they did, Envestnet should not put the burden on consumers to locate a notice buried in small print in a bank's or apps' [sic] terms and conditions . . . in order [to] protect their privacy.

The authors argued that FTC policy prohibits "hid[ing] important facts about how consumer data is collected or shared in the small print of a privacy policy" and FTC has stated that, "companies have an obligation to disclose 'facts [that] would be material to consumers in deciding to install the software.'"

---

[34] *See* Wyden, *supra* n.1.

[35] *Id.*

[36] *Id.*

136. According to Envestnet's Form 10-K for the 2019 fiscal year, in February 2020, the FTC issued a civil investigative demand to Envestnet for various documents related to this matter. Envestnet itself recognizes the risk that as a result of the FTC's investigation, proceedings may be initiated and they may be found to have violated applicable laws, which could have a material adverse effect on their operations and financial condition. Envestnet reported in its Form 10-K for the 2020 fiscal year that the FTC had closed the matter.

TOLLING, CONCEALMENT AND ESTOPPEL

137. The statutes of limitation applicable to Plaintiffs' claims are tolled as a result of Yodlee's knowing and active concealment of their conduct alleged herein. Among other things, Yodlee designs its software to deceive users into thinking that they are interacting directly with their banks when providing log in credentials to facilitate a connection between their bank accounts and a third-party service. Yodlee also fails to disclose to each individual user—either through their own privacy policy, website, or other document—that they store the bank log in information provided in such log in transactions and use those credentials to collect financial data from the individual's bank accounts on an ongoing basis, even though the individual never consented to such data collection. Nor does Yodlee inform each individual user that this data collection will continue even if the individual revokes the permissions granted to the third-party service it sought to connect to her bank account. By these actions, Yodlee intentionally concealed the nature and extent of its data collection operation to maximize profits resulting from the sale of Plaintiffs' and Class members' highly sensitive financial information. To the extent Yodlee's customers or others made statements regarding Yodlee's service or privacy policies, Yodlee either approved those inadequate statements or failed to timely correct them in service of their ongoing scheme to conceal the true nature of its conduct.

138. Plaintiffs and Class members could not, with due diligence, have discovered the full scope of Yodlee's conduct, due to Yodlee's deliberate efforts to conceal it. All applicable statutes of limitation also have been tolled by operation of the discovery rule. Under the circumstances, Yodlee was under a duty to disclose the nature and significance of their data and privacy policies and practices but did not do so. Yodlee therefore is estopped from relying on any statute of

limitations.

139. Further, this Complaint alleges a continuing course of unlawful conduct by which Yodlee has inflicted continuing and accumulating harm within the applicable statutes of limitations.

140. Each time Yodlee engaged in an unlawful act complained of here, Yodlee undertook an overt act that has inflicted harm on Plaintiffs and other members of the Classes.

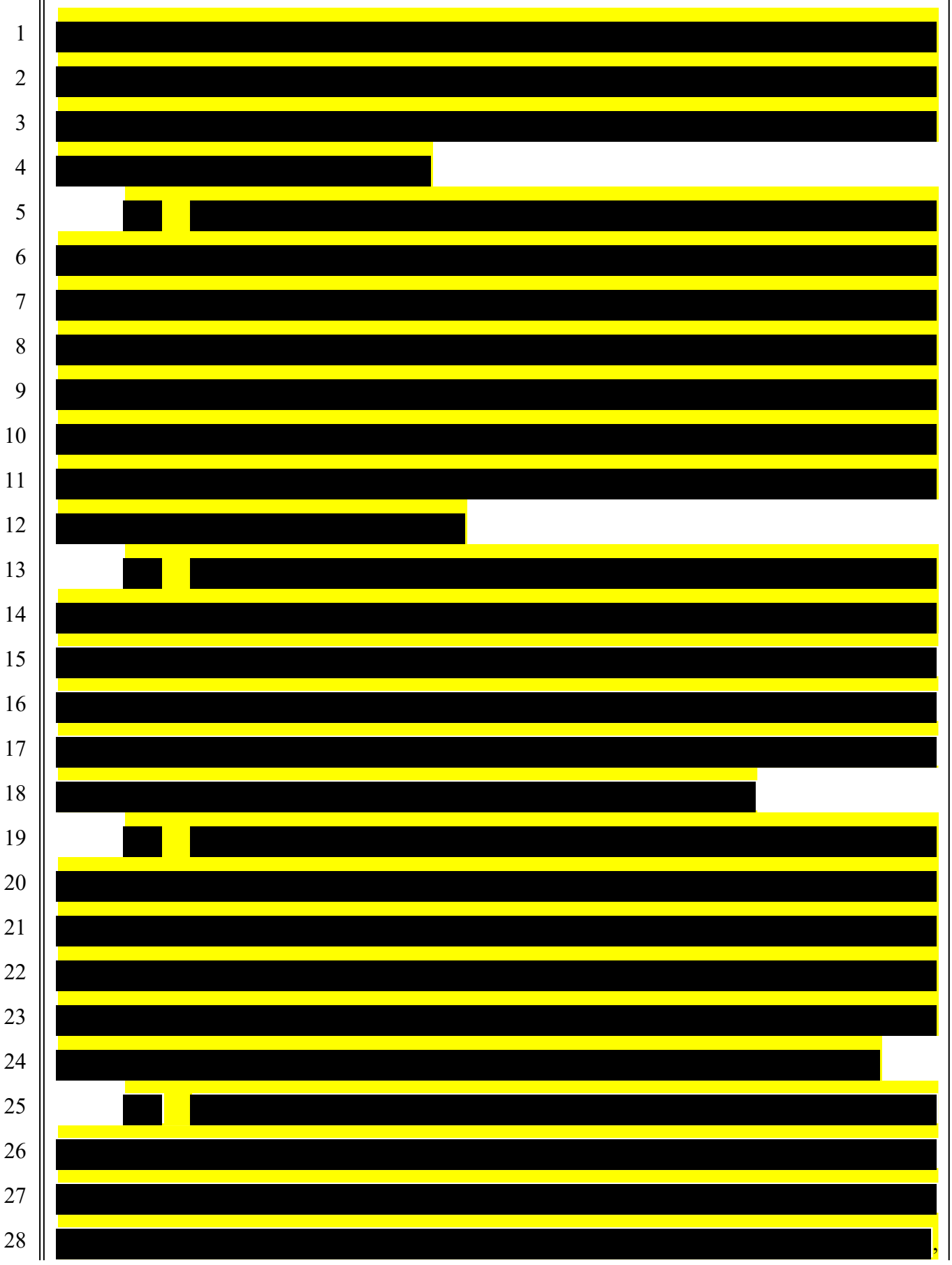
141. For these reasons, the statutes of limitations have been tolled with respect to the claims of Plaintiffs and members of the Classes asserted in this Complaint.

142. Yodlee's fraudulent concealment and omissions are common to Plaintiffs and all Class members.

PLAINTIFFS LACK AN ADEQUATE REMEDY AT LAW

143. Plaintiffs lack an adequate remedy at law and therefore are entitled to disgorge Yodlee's unjust profits because damages alone are inadequate to recoup the unjust profits and benefits Yodlee gained from exploiting Plaintiffs' and Class members' data. Because Yodlee has monetized Plaintiffs' data in ways that do not involve Plaintiffs, and do not necessarily give rise to damages, Yodlee's unjust profits are not coextensive with, and may exceed, Plaintiffs' compensatory damages.

[redacted]



[redacted] Yodlee continues to retain those benefits, and absent a disgorgement remedy, would stand to unjustly retain those benefits to the extent they exceed the amount of Plaintiffs' and Class members' damages.

152. Plaintiffs therefore do not have an adequate remedy at law because monetary damages alone are not sufficient to recoup Yodlee's unjust profits.

CLASS ACTION ALLEGATIONS

153. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Classes:

> **Nationwide Class:** All natural persons in the United States whose accounts at a financial institution were accessed by Yodlee using login credentials obtained through Yodlee's software incorporated in a mobile or web-based fintech app that enables payments (including ACH payments) or other money transfers from 2014 through the present.
>
> **California Class:** All natural persons in California whose accounts at a financial institution were accessed by Yodlee using login credentials obtained through Yodlee's software incorporated in a mobile or web-based fintech app that enables payments (including ACH payments) or other money transfers from 2014 through the present.

154. Excluded from each of the Classes are: (1) any Judge or Magistrate presiding over this action and any members of their families; (2) Yodlee, Yodlee's subsidiaries, parents, successors, predecessors, and any entity in which a Defendant or its parent has a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiffs' counsel and Yodlee's counsel.

155. **Numerosity:** The exact number of members of the Classes is unknown and unavailable to Plaintiffs at this time, but individual joinder in this case is impracticable. The Classes

likely consist of millions of individuals, and the members can be identified through Yodlee's records.

156. **Predominant Common Questions:** The Classes' claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class members. Common questions for the Classes include, but are not limited to, the following:

a. Whether Yodlee violated Plaintiffs' and Class members' privacy rights;

b. Whether Yodlee's acts and practices complained of herein amount to egregious breaches of social norms;

c. Whether Yodlee's conduct was negligent;

d. Whether Yodlee's conduct was unlawful;

e. Whether Yodlee's conduct was unfair;

f. Whether Yodlee's conduct was fraudulent;

g. Whether Plaintiffs and the Class members are entitled to equitable relief, including but not limited to, injunctive relief, restitution, and disgorgement;

h. Whether Plaintiffs and the Class members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief; and

i. Whether Plaintiffs and the Class members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

157. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of the Classes. The claims of Plaintiffs and the members of the Classes arise from the same conduct by Yodlee and are based on the same legal theories.

158. **Adequate Representation:** Plaintiffs have and will continue to fairly and adequately represent and protect the interests of the Classes. Plaintiffs have retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiffs have no interest that is antagonistic to those of the Classes, and Yodlee has no defenses unique to any Plaintiff. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and they have the resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of

the Classes.

159. **Substantial Benefits:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Classes is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

160. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CALIFORNIA LAW APPLIES TO THE NATIONWIDE CLASS

161. California's substantive laws apply to every member of the Nationwide Class, regardless of where in the United States the Class member resides. The State of California has sufficient contacts to Yodlee's relevant conduct for California law to be uniformly applied to the claims of the Nationwide Class.

162. Further, California's substantive laws may be constitutionally applied to the claims of Plaintiffs and the Nationwide Class under the Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV § 1 of the U.S. Constitution. California has significant contacts, or significant aggregation of contacts, to the claims asserted by Plaintiffs and all Class members, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair.

163. Envestnet | Yodlee's headquarters and principal place of business is located in California. Yodlee also own property and conduct substantial business in California, and therefore California has an interest in regulating Yodlee's conduct under its laws. Yodlee's conduct originated in, and emanated from, California and impacted a significant percentage of California residents, rendering the application of California law to the claims here constitutionally permissible.

164. The application of California laws to the Nationwide Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiffs

and the proposed Nationwide Class, and California has a greater interest in applying its laws here than any other interested state.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiffs and the Classes)

165. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

166. Yodlee intruded upon Plaintiffs and Class members' seclusion by (1) collecting and selling their sensitive personal data in which they had a reasonable expectation of privacy; and (2) in a manner that was highly offensive to Plaintiffs and Class members, would be highly offensive to a reasonable person, and was an egregious violation of social norms.

167. Yodlee's conduct violated Plaintiffs' and Class members' interests by collecting, selling, and otherwise misusing their sensitive personal data, including information concerning private financial transactions (i.e., their informational privacy rights), as well as their interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference (i.e., their autonomy privacy rights). Yodlee's conduct is especially egregious as they fail to have any adequate security measures in place to control what their clients do with Plaintiffs' and Class members' information once it is sold, such as re-identifying Plaintiffs and Class members or using it for nefarious purposes.

168. The surreptitious taking and disclosure of personal, confidential, and private information from millions of individuals was highly offensive because it violated expectations of privacy that have been established by general social norms.

169. Polls and studies consistently show that the overwhelming majority of Americans believe one of the most important privacy rights is the need for an individual's affirmative consent before personal data is shared. For example, one study by *Pew Research* found that 93% of Americans believe it is important to be in control of who can get information about them.

170. Yodlee's conduct would be highly offensive to a reasonable person in that it violated

federal and state laws designed to protect individual privacy, in addition to social norms.

171. Yodlee intentionally engaged in the misconduct alleged herein for their own financial benefit unrelated to any service they provide. Specifically, Yodlee collected and sold Plaintiffs' and Class members' lucrative (and private) sensitive information for their own financial benefit.

172. As a result of Yodlee's actions, Plaintiffs and Class members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

173. Plaintiffs and Class members have been damaged as a direct and proximate result of Yodlee's invasion of their privacy and are entitled to just compensation.

174. Plaintiffs and Class members are entitled to appropriate relief, including compensatory damages for the harm to their privacy and dignitary interests, loss of valuable rights and protections, heightened risk of future invasions of privacy, and mental and emotional distress.

175. Plaintiffs and Class members are entitled to an order requiring Yodlee to disgorge profits or other benefits that Yodlee acquired from their misconduct to the extent those profits or benefits exceed Plaintiffs' and Class members' damages.

176. Plaintiffs and Class members also seek injunctive and other equitable relief. They do not have an adequate remedy at law because: (1) an award of damages will not encompass the profits Yodlee unjustly earned from its unauthorized sale and use of their highly sensitive financial data, and (2) many of the resulting injuries are reoccurring, and Plaintiffs and Class members will be forced to bring multiple lawsuits to rectify the same conduct. As for injunctive relief, if an injunction is not issued, Plaintiffs and Class members will suffer irreparable injury. Plaintiffs and Class members are entitled to an order requiring Yodlee to disgorge any profits unjustly earned from its unauthorized sale and use of Plaintiffs' and Class members' data to the extent they exceed Plaintiffs' damages, enjoining Yodlee from engaging in the unlawful conduct alleged in this complaint, requiring Yodlee to delete Plaintiffs' and Class members' sensitive personal data, requiring Yodlee to cease further collection of Plaintiffs' and Class members' sensitive personal data, requiring Yodlee to improve its privacy disclosures, requiring Yodlee to obtain adequately informed consent, and other appropriate equitable relief.

177. Plaintiffs and Class members are entitled to punitive damages resulting from the malicious, willful and intentional nature of Yodlee's actions, directed at injuring Plaintiffs and Class members in conscious disregard of their rights. Such damages are needed to deter Yodlee from engaging in such conduct in the future.

178. Plaintiffs also seek such other relief as the Court may deem just and proper.

SECOND CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiffs and the Classes)

179. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

180. Yodlee received benefits from Plaintiffs and Class members and unjustly retained those benefits at their expense.

181. In particular, Yodlee received benefits from Plaintiffs and Class members in the form of the sensitive personal data that Yodlee collected from Plaintiffs and Class members, without authorization and proper compensation. Yodlee has collected, sold, and otherwise misused this information, for its own gain, providing Yodlee with economic, intangible, and other benefits, including substantial monetary compensation from the entities who purchased Plaintiffs' and Class members' sensitive personal data.

182. Yodlee unjustly retained those benefits at the expense of Plaintiffs and Class members because Yodlee's conduct damaged Plaintiffs and Class members, all without providing any commensurate compensation to Plaintiffs and Class members.

183. The benefits that Yodlee derived from Plaintiffs and Class members rightly belong to Plaintiffs and Class members. It would be inequitable under unjust enrichment principles in California and every other state for Yodlee to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

184. Plaintiffs and Class members also seek injunctive relief. They do not have an adequate remedy at law because many of the resulting injuries are reoccurring, and Plaintiffs and

Class members will be forced to bring multiple lawsuits to rectify the same conduct. If an injunction is not issued, Plaintiffs and Class members will suffer irreparable injury. Plaintiffs and Class members are entitled to an order enjoining Yodlee from engaging in the unlawful conduct alleged in this complaint, requiring Yodlee to delete Plaintiffs' and Class members sensitive personal data, requiring Yodlee to cease further collection of Plaintiffs' and Class members sensitive personal data, requiring Yodlee to improve its privacy disclosures, requiring Yodlee to obtain adequately informed consent, and other appropriate equitable relief.

185. Yodlee should be compelled to disgorge in a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds they received to the extent they exceed Plaintiffs' damages, and such other relief as the Court may deem just and proper.

THIRD CLAIM FOR RELIEF
Violation of California's Anti-Phishing Act of 2005
Cal. Bus. & Prof. Code § 22948.2
(On Behalf of Plaintiffs and the Classes)

186. Plaintiffs incorporate the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

187. Plaintiffs brings this claim on behalf of themselves and the Nationwide Class or, in the alternative, the California Class.

188. The California Anti-Phishing Act of 2005 (the "Anti-Phishing Act") makes it unlawful to use the Internet "to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business." Cal. Bus. & Prof. Code § 22948.2. "Identifying information" includes bank account numbers, account passwords, and "[a]ny other piece of information that can be used to access an individual's financial accounts." Cal. Bus. & Prof. Code § 22948.1(b). An individual who is adversely affected by a violation of Section 22948.2 may bring an action. Cal. Bus. & Prof. Code § 22948.3(a)(2).

189. As described herein, Yodlee violated the Anti-Phishing Act by representing themselves to be Plaintiffs' and Class members' financial institutions. Yodlee fraudulently and deceitfully impersonated those institutions in order to induce Plaintiffs and Class members to

provide their login credentials to Yodlee, as described herein. Yodlee did so without obtaining the authority or approval of each financial institution.

190. Plaintiffs and Class members have been adversely affected by Yodlee's violations of the Anti-Phishing Act because Yodlee engaged in this deceitful conduct in order to extract from Plaintiffs and Class members their login credentials and all of the transaction history and other data accessible with those credentials, as detailed above. Yodlee caused actual injury, harm, damage and loss to Plaintiffs and Class members for the reasons described herein.

191. Plaintiffs and Class members are entitled to relief under Cal. Bus. & Prof. Code § 22948.3(a)(2), including $5,000 per violation, which damages should be trebled because Yodlee engaged in a pattern and practice of violating § 22948.2 (indeed, it is the essence of Yodlee's business model); an injunction against further violations; costs of suit and reasonable attorney's fees; and such other relief as the Court may deem just and proper.

FOURTH CLAIM FOR RELIEF
Violation of Article I, Section I of the California Constitution
(On Behalf of Plaintiff Szeto and the California Class)

192. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

193. The California Constitution expressly provides for and protects the right to privacy of California citizens: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const., art. I, § 1.

194. Plaintiff Szeto and members of the California Class have a reasonable expectation of privacy in their confidential financial affairs, including without limitation in the personal information and banking data maintained at their financial institutions. Plaintiffs and California Class members reasonably expected that their login credentials, account numbers, balances, transaction history, and other information was private and secure within the institutions at which they maintain accounts. They reasonably expected that their information and data (a) would be protected and secured against access by unauthorized parties; (b) would not be obtained by

unauthorized parties; (c) would not be transmitted or stored outside of the secure bank environment; and (d) would not be sold or used without their knowledge or permission.

195. Plaintiff Szeto and California Class members have a legally protected privacy interest in preventing the unauthorized access, dissemination, sale, and misuse of their sensitive and confidential banking information and data.

196. Yodlee intentionally violated Plaintiff Szeto and California Class members' privacy interests. Yodlee intruded upon Plaintiff Szeto and California Class members' sensitive and confidential banking information in a manner sufficiently serious in nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right.

197. Yodlee intentionally violated Plaintiff Szeto and California Class members' privacy interests by improperly accessing, downloading, transferring, selling, storing and using their private banking information and data.

198. Yodlee's violations of Plaintiffs' and California Class members' privacy interests would be highly offensive to a reasonable person, especially considering (a) the highly sensitive and personal nature of Plaintiffs' and California Class members' banking information and data; (b) the extensive scope of data obtained by Yodlee, including years of historical transactional data; (c) Yodlee's intent to profit from Plaintiffs' and California Class members' data by selling it outright and using it to develop further products and services; and (d) the fact that Yodlee used subterfuge to intrude into Plaintiffs' and California Class members' banks' secure environment for the purpose of collecting their data. Yodlee's intrusions were substantial and constituted an egregious breach of social norms.

199. Plaintiff Szeto and California Class members did not consent to Yodlee's violations of their privacy interests.

200. Plaintiff Szeto and California Class members suffered actual and concrete injury as a result of Yodlee's violations of their privacy interests. Plaintiffs and California Class members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by

Yodlee's invasions, as well as disgorgement of profits made by Yodlee as a result of its violations of their privacy interests to the extent those profits or benefits exceed Plaintiffs' and Class members' damages.

201. Plaintiffs and Class members also seek injunctive and other equitable relief. They do not have an adequate remedy at law because: (1) an award of damages will not encompass the profits Yodlee unjustly earned from its unauthorized sale and use of their highly sensitive financial data, and (2) many of the resulting injuries are reoccurring, and Plaintiffs and Class members will be forced to bring multiple lawsuits to rectify the same conduct. As for injunctive relief, if an injunction is not issued, Plaintiffs and Class members will suffer irreparable injury. Plaintiffs and Class members are entitled to an order requiring Yodlee to disgorge any profits unjustly earned from its unauthorized sale and use of Plaintiffs' and Class Members' data to the extent they exceed Plaintiffs' damages, enjoining Yodlee from engaging in the unlawful conduct alleged in this complaint, requiring Yodlee to delete Plaintiffs' and Class members' sensitive personal data, requiring Yodlee to cease further collection of Plaintiffs' and Class members' sensitive personal data, requiring Yodlee to improve its privacy disclosures, requiring Yodlee to obtain adequately informed consent, and other appropriate equitable relief.

202. Plaintiff Szeto and California Class members also seek punitive damages because Yodlee's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and California Class members and made in conscious disregard of Plaintiffs' and California Class members' rights. Punitive damages are warranted to deter Yodlee from engaging in future misconduct.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and the proposed Classes respectfully request that the Court enter an order:

A. Certifying the Classes and appointing Plaintiffs as Class Representatives;

B. Finding that Yodlee's conduct was unlawful as alleged herein;

C. Awarding declaratory relief against Yodlee;

D. Awarding such injunctive and other equitable relief as the Court deems just and

proper;

E. Awarding Plaintiffs and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

F. Awarding Plaintiffs and the Class members pre-judgment and post-judgment interest;

G. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses, including expert costs;

H. Granting injunctive and other equitable relief because Plaintiffs and Class members do not have an adequate remedy at law; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Dated: September 19, 2023

/s/ Christian Levis

Christian Levis (*pro hac vice*)
Amanda Fiorilla (*pro hac vice*)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

Anthony M. Christina (*pro hac vice*)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Facsimile: (914) 997-0035
achristina@lowey.com

Ben Steinberg (*pro hac vice*)
Kellie Lerner (*pro hac vice* forthcoming)
ROBINS KAPLAN LLP
1325 Avenue of the Americas, Suite 2601
New York, NY 10019
Telephone: (212) 980-7400
Facsimile: (212) 980-7499
klerner@robinskaplan.com
bsteinberg@robinskaplan.com

Li Zhu (SBN 302210)
ROBINS KAPLAN LLP
55 Twin Dolphin Drive, Suite 310
Redwood City, CA 94065-2133
Telephone: (605) 784-4013
lzhu@robinskaplan.com

Thomas J. Undlin (*pro hac vice* forthcoming)
ROBINS KAPLAN LLP
800 LaSalle Avenue, Suite 2800
Minneapolis, MN 55402
Telephone: (612) 349-8500
Facsimile: (612) 339-4181
tundlin@robinskaplan.com

John Emerson
EMERSON FIRM, PLLC
2500 Wilcrest Drive
Suite 300
Houston, TX 77042
Telephone: (800) 551-8649
Facsimile: (501) 286-4659
jemerson@emersonfirm.com

Robert Kitchenoff (*pro hac vice* forthcoming)
WEINSTEIN KITCHENOFF & ASHER LLC
150 Monument Road, Suite 107
Bala Cynwyd, PA 19004
Telephone: (215) 545-7200
kitchenoff@wka-law.com

Michele Carino (pro hac vice forthcoming)
GREENWICH LEGAL ASSOCIATES LLC
881 Lake Avenue
Greenwich, CT 06831
Telephone: (203) 622-6001
mcarino@grwlegal.com

Attorneys for Plaintiffs and the Proposed Classes